Claims

1. Method for managing certificates in a certificate authority in a system having at least a first plurality of certificate authorities, comprising at least the step of

generating at least two certificate revocation lists of a first type,

each of said at least two certificate revocation lists of a first type not indicating a revoked status of any certificate authority in said at least a first plurality of certificate authorities,

said at least two certificate revocation lists of a first type having at least partially consecutive validity periods,

where the beginning of the validity period of at least one of said at least two certificate revocation lists of a first type is a future point of time.

2. Method according to claim 1, comprising at least the steps of

publishing said certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

3. Method according to claim 1, comprising at least the steps of

checking regarding each of certificate authorities listed in said certification revocation lists of a first type if the security of each of certificate authorities has been breached or not;

and if the security of none of said certificate authorities has been breached, publishing one of said certificate revocation lists of a first type.

4. Method according to claim 1, comprising at least the steps of

generating at least two certificate revocation lists of a second type,

each of said at least two certificate revocation lists of a second type indicating a revoked status of at least one certificate authority in said at least a first plurality of certificate authorities,

said at least two certificate revocation lists of a second type having at least partially consecutive validity periods,

where the beginning of the validity period of at least one of said at least two certificate revocation lists of a second type is a future point of time.

5. Method according to claim 4, comprising at least the steps of

checking regarding each of certificate authorities in said at least a first plurality of certificate authorities if the security of each of certificate authorities has been breached or not;

and if the security of none of said certificate authorities has been breached, publishing one of said certificate revocation lists of a first type,

and if the security of at least one of said certificate authorities has been breached, publishing one of said certificate revocation lists of a second type.

6. Method according to claim 4, comprising at least the steps of

generating for each certificate authority in said at least a first plurality of certificate authorities if the security of each of certificate a series of certificate revocation lists which indicate a revoked status of said certificate authority.

7. Method according to claim 1, comprising at least the steps of

generating at least two certificate revocation lists of a third type,

each of said at least two certificate revocation lists of a third type indicating a temporarily suspended status of at least one certificate authority in said at least a first plurality of certificate authorities,

said at least two certificate revocation lists of a third type having at least partially consecutive validity periods,

where the beginning of the validity period of at least one of said at least two certificate revocation lists of a third type is a future point of time.

8. System for a certificate authority having means for generating certificate revocation lists, comprising at least

means for generating sequences of certificate revocation lists of a first type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a first type being a future point of time relative to the time of generating a sequence of certificate revocation lists,

said certificate revocation lists of a first type indicating no revocation for a predefined group of certificate authorities.

9. System according to claim 8, further comprising at least means for publishing said certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

10. System according to claim 8, comprising at least

means for generating sequences of certificate revocation lists of a second type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a second type being a future point of time relative to the time of generating a sequence of certificate revocation lists, and

means for generating an indication of a revoked status of at least one certificate authority in said predefined group of certificate authorities in each certificate revocation list generated by said means for generating sequences of certificate revocation lists of a second type.

11. System according to claim 10, comprising at least

means for checking regarding each of certificate authorities in said predefined group of certificate authorities if the security of each of said certificate authorities has been breached or not;

means for publishing one of said certificate revocation lists of a first type if the security of none of said certificate authorities has been breached, and

means for publishing one of said certificate revocation lists of a second type if the security of at least one of said certificate authorities has been breached.

12. Computer program product for a certificate authority having computer code means for generating certificate revocation lists, comprising at least

computer program code means for generating sequences of certificate revocation lists of a first type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a first type being a future point of time relative to the time of generating a sequence of certificate revocation lists,

said certificate revocation lists of a first type indicating no revocation for a predefined group of certificate authorities.

13. Computer program product according to claim 12, comprising at least computer program code means for publishing said certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

14. Computer program product according to claim 12, comprising at least

computer program code means for generating sequences of certificate revocation lists of a second type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a second type being a future point of time relative to the time of generating a sequence of certificate revocation lists, and

computer program code means for generating an indication of a revoked status of at least one certificate authority in said predefined group of certificate authorities in each certificate revocation list generated by said means for generating sequences of certificate revocation lists of a second type.

15. Computer program product according to claim 14, comprising at least

computer program code means for checking regarding each of certificate authorities in said predefined group of certificate authorities if the security of each of said certificate authorities has been breached or not;

computer program code means for publishing one of said certificate revocation lists of a first type if the security of none of said certificate authorities has been breached, and

computer program code means for publishing one of said certificate revocation lists of a second type if the security of at least one of said certificate authorities has been breached.